

CHAPTER 10 الفصل العاشر
FIREWALLS جدران النار

مبادئ تصميم جدران النار Firewall Design Principles
خصائص جدار النار Firewall Characteristics
أنواع جدران النار Types of Firewalls
تهيئات جدار النار Firewall Configurations

مقدمة:
يمكن أن تكون جدران النار (Firewalls) وسائل فعالة في حماية أي نظام محلي أو شبكة أنظمة من المهددات الأمنية المعتمدة على الشبكات (Network-based security threats) ، في حين أنها في نفس الوقت تتحمل مسئولية الوصول إلى العالم الخارجي عبر شبكات الـ (Wide Area Networks) (WANs) ، و كذلك عبر شبكة الإنترنت.

مبادئ تصميم جدران النار (Firewall Design Principles):
مرت أنظمة المعلومات في الشركات ، و الوكالات الحكومية ، و المنظمات الأخرى بتطور ثابت كما هو مبين أدناه :

- نظام معالجة البيانات المركزية (Centralized data processing system) ، و الذي يحتوي على حاسب ضخم مركزي (central mainframe) يدعم العديد من الطرفيات (terminals) المتصلة مباشرة.
- الشبكات المحلية (LANs) ، و التي تزود بربط داخلي لأجهزة الحاسوب الشخصية (PCs) و الطرفيات مع بعضها البعض و كذلك مع الـ (mainframe).
- الشبكة الفرضية (Premises network) ، و تتكون من عدد من الـ (LANs) ، و تزود بالربط الداخلي لكل من الـ (PCs) و الـ (servers) و ربما الـ (mainframe) أو كليهما.
- شبكة المشروع العريض (Enterprise-wide network) ، وتتكون من العديد من الـ (promises networks) الموزعة جغرافياً و المتصلة داخلياً عن طريق شبكات الوان الخاصة (Private Wide Area Network).
- ربط الإنترنت (Internet connectivity) ، و فيه ترتبط العديد من الـ (Premises networks) عن طريق الإنترنت و هي قد تتصل أو قد لا تتصل بـ (private WAN).

أهداف جدار النار (Firewall aims):
- يؤسس إرتباط يمكن التحكم به (Establish a controlled link).
- يحمي الـ (premises network) من الهجمات المعتمدة على الإنترنت (Internet-based attacks).
- يزود بنقطة اختناق (single choke point) .

خصائص جدار النار (Firewall Characteristics):
الأهداف التصميمية (Designing Goals):
هناك مجموعة من الأهداف التصميمية لـ (Firewalls) يمكن سردها فيما يلي :
1- كل عمليات المرور (traffic) من الداخل إلى الخارج ، و العكس ، يجب أن تمر عبر الـ (Firewall). ويمكن إنجاز هذا المفهوم عن طريق المنع الفيزيائي (blocking) لكل عمليات الوصول للشبكة المحلية إلا عبر الـ (Firewall).



2- الـ (traffic) المصرح له (كما هو معرف في سياسة السرية المحلية) هو فقط من سيسمح له بالمرور. هناك أنواع عديدة من الـ (Firewalls) المستخدمة ، و التي تنفذ أنواع مختلفة من سياسات السرية (security policies).
3- يكون الـ (Firewall) ذات نفسه محصناً ضد عمليات الإختراق (penetration). و هذا يقتضي إستخدام نظام موثوق به (Trusted system) مع نظام تشغيل آمن (Secure O.S.).

تقنيات جدار النار المستخدمة للتحكم بالوصول وفرض سياسات السرية (Firewall techniques used to control access and enforce security policy):

هناك أربع تقنيات عامة تستخدمها الـ (Firewalls) للتحكم بالوصول و تمكين سياسات السرية المعرفة من قبل موقع معين، و سنشرحها فيما يلي:

1- **خدمة التحكم (Service control):**
و هي خدمة تحدد أنواع خدمات الإنترنت (Internet services) التي يمكن الوصول إليها. حيث يقوم الـ (Firewall) بعمل تنقية لـ (traffic) اعتماداً على عنوان الـ (IP) و كذلك رقم الـ (TCP port)؛ أو قد يزود الـ (Firewall) ببرمجية (Proxy) مهمتها استقبال و تفسير كل طلب من طلبات الخدمة قبل تمريره؛ أو قد يستضيف الـ (Firewall) برمجية الـ (Server) نفسها كما هو الحال في خدمات الـ (Web) و البريد الإلكتروني (E-mail).

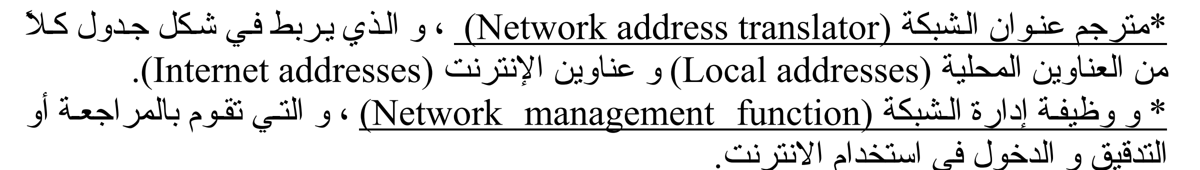
2- **التحكم بالاتجاه (Direction control):**
و هي تقنية تحدد الاتجاه الذي يمكن أن تبدأ طلبات خدمة معينة بسلوكه ، حيث يسمح لها بالمرور عبره لاجتياز الـ (Firewall) .

3- **التحكم بالمستخدم (User control):**
و هي تقنية الغرض منها التحكم بالوصول إلى الخدمة اعتماداً على ماهية المستخدم الذي يحاول الوصول إليها. و هذه الميزة تطبق أيضاً على المستخدمين الموجودين على حافة الـ (Firewall) (أو ما نطلق عليهم بالمستخدمين المحليين). يمكن أن تطبق أيضاً على الـ (traffic) القادم من المستخدمين الخارجيين و هنا قد يتطلب الأمر وجود تكنولوجيا التحقق الآمن.

4- **التحكم بالسلوك (Behavior control):**
و تتحكم هذه التقنية بكيفية استخدام الخدمات. مثلاً ، قد يقوم الـ (Firewall) بعمل تنقية للبريد الإلكتروني (E-mail) للتخلص من الرسائل الغير حقيقية ، أو أن الـ (Firewall) قد يقوم بتمكين الوصول الخارجي فقط لجزء من المعلومات على خادم وب محلي.

مقدرات جدار النار (Capabilities of Firewall):

1- يمكن لـ (Firewall) أن يعرف نقطة اختناق (Choke point) ، و هي تحتفظ بالمستخدمين الغير مصرح لهم بالوصول بعيداً عن الشبكة المحمية، و تمنع الخدمات الهشة من دخول أو مغادرة الشبكة، و تزود بالحماية ضد الأنواع المختلفة لهجمات الـ (IP) مثل التزوير في بروتوكول الإنترنت (IP spoofing) أو تغيير مسار بروتوكول الإنترنت (IP routing). إن استخدام (choke point) وحيدة يبسط عملية إدارة السرية (security management) و ذلك لأن إمكانيات السرية مدعومة سواءً في نظام وحيد أو مجموعة من الأنظمة.
2- يزود الـ(Firewall) بموقع لمراقبة الأحداث التي لها علاقة بالسرية . يمكن تنفيذ مراجعة و تدقيق الحسابات (Audits) و كذلك أجراس الإنذار (Alarms) على نظام الـ (Firewall).
3- يعد الـ (Firewall) بيئة ملائمة للعديد من وظائف الإنترنت (Internet functions) التي لها علاقة بالسرية. من الأمثلة على ذلك :



*مترجم عنوان الشبكة (Network address translator) ، و الذي يربط في شكل جدول كلاً من العناوين المحلية (Local addresses) و عناوين الإنترنت (Internet addresses).
* و وظيفة إدارة الشبكة (Network management function) ، و التي تقوم بالمراجعة أو التدقيق و الدخول في استخدام الانترنت.

4- يمكن أن يعمل الـ (Firewall) كبيئة لسرية بروتوكول الانترنت (IPSec) . حيث أنه باستخدام الـ (Tunnel mode) الذي شرحناه في الفصل السادس يمكن للـ (Firewall) تنفيذ شبكة إفتراضية خاصة (Virtual private network).

محدوديات (أوجه القصور) في جدار النار (Firewall limitations):

1- لايمكن للـ (Firewall) أن يزود بالحماية ضد تلك الهجمات التي اجتازت جدار النار. قد تمتلك الأنظمة الخارجية خاصية الـ (Dial-out) للاتصال بمزود خدمة الإنترنت (ISP). يمكن أن تدعم شبكة الـ (LAN) الداخلية بـ (modem pool) للتزويد بخاصية الـ (Dial-in) للموظفين المتنقلين.
2- لا يزود الـ (Firewall) بالحماية ضد المهددات الداخلية ، مثال على ذلك الهجمهات التي يتعاون فيها الموظفون الساخطون من داخل المؤسسة مع مهاجمين خارجيين.
3- لا يزود الـ (Firewall) بالحماية ضد انتقال البرامج أو الملفات المعدية بالفيروسات. و قد يكون من غير العملي و ربما من المستحيل على الـ (Firewall) أن يفحص كل الملفات , و الإيميلات ، و الرسائل القادمة من أجل التأكد من وجود فيروسات ، و لعل السبب في ذلك وجود العديد من أنظمة التشغيل و التطبيقات المدعومة داخل نطاق الـ (Firewall).

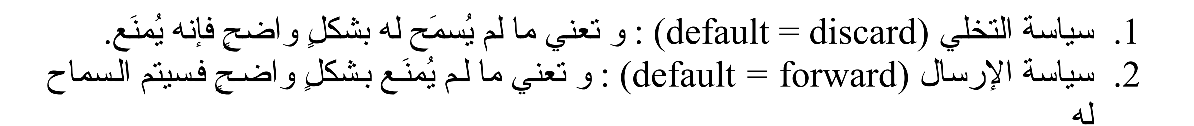
أنواع جدران النار(Types of Firewalls):

هناك ثلاثة أنواع شائعة من جدران النار ، و هي :

1. مسيرات تنقية الحزمة (Packet-filtering routers).
2. بوابات المستوى التطبيقي (Application-level gateways).
3. بوابات على مستوى الدائرة (Circuit-level gateways).

النوع الأول : مسيرات تنقية الحزمة (Packet-filtering routers):

- تقوم بتطبيق مجموعة من القواعد على كل (IP packet) قادمة و من ثم إرسال هذه الـ (packet) أو التخلي عنها.
- يتم تهيئة الـ (router) بحيث يقوم بعمل تنقية للـ (packets) المرسلة في كلا الاتجاهين (من و إلى الشبكة الداخلية).
- تعتمد قواعد التنقية (Filtering rules) على مطابقتها لبعض الحقول في الـ (IP header) و الـ (TCP header)، حيث يتم نداء تلك الـ (rule) لتحديد فيما إذا كان يجب إرسال الـ (packet) أو التخلي عنها. من الأمثلة على هذه الحقول :
  1. عنوان بروتوكول الانترنت للمصدر (source IP address).
  2. عنوان بروتوكول الانترنت للوجهة (destination IP address).
  3. حقل بروتوكول الانترنت (IP protocol field) ، و هذا الحقل يعرف بروتوكول النقل (Transport protocol).
  4. رقم الـ (port) للـ (TCP) أو للـ (UDP)، و هو يعرف التطبيق مثل بروتوكول SNMP أو TELNET.
- إذا لم يكن هناك أي تطابق مع أي (rule)، فسيتم حينها إتخاذ حدث إفتراضي (default action)، هناك سياستان افتراضيتان ممكنتان هما:



1. سياسة التخلي (default = discard) : و تعني ما لم يُسمَح له بشكلٍ واضح فإنه يُمنَع.
2. سياسة الإرسال (default = forward) : و تعني ما لم يُمنَع بشكلٍ واضحٍ فسيتم السماح له.

خصائص الـ (default discard):

- محافظة أكثر، حيث يتم عمل (blocking) لكل شئ و يجب إضافة الخدمات على قاعدة (case-by-case).
- مرئية أكثر بالنسبة للمستخدمين، حيث من الراجح انهم يرون جدار النار كالعائق.

خصائص الـ (default forward) :

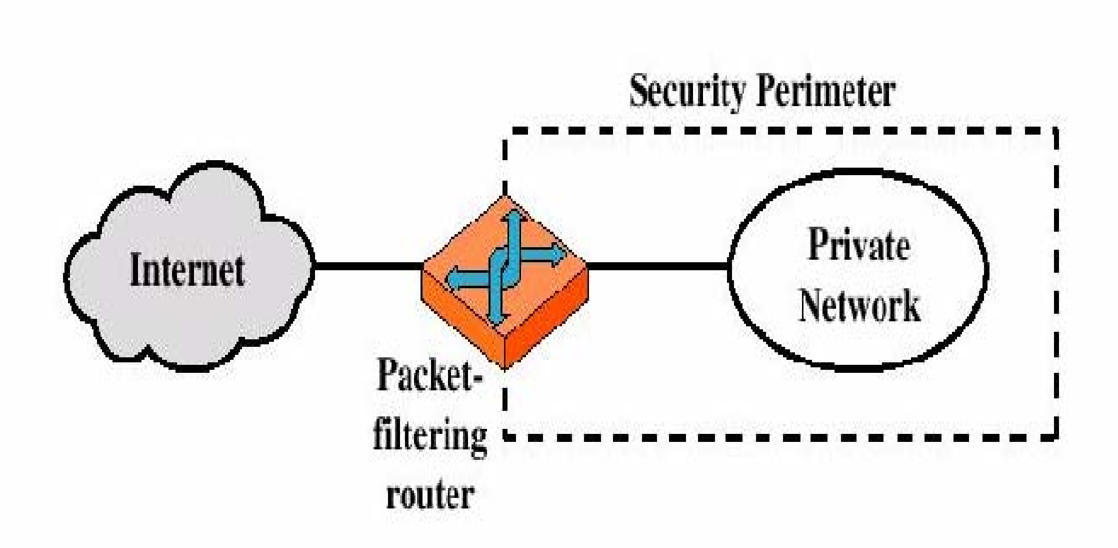
- تزيد من سهولة الاستخدام بالنسبة للـ (end users).
- يمنح سرية أقل.

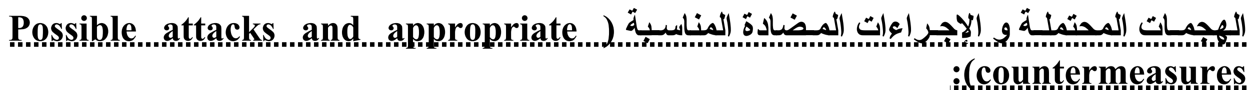
مزايا مسيرات تنقية الحزمة (Advantages of Packet-Filtering Router):

- البساطة (Simplicity).
- الشفافية بالنسبة للمستخدمين (Transparency to users).
- السرعة العالية (High speed).

مساوئ مسيرات تنقية الحزمة (Disadvantages of Packet-Filtering Router):

- صعوبة وضع قواعد تنقية الحزمة (Difficulty of setting up packet filter rules).
- نقص التحققية (Lack of Authentication).





الهجمات المحتملة و الإجراءات المضادة المناسبة (Possible attacks and appropriate countermeasures):

الهجمة الأولى : التزوير في عنوان بروتوكول الانترنت (IP address spoofing):

- يقوم الدخيل (intruder) بإرسال الـ (packets) من الخارج بحيث يحتوي حقل الـ (source IP address) على عنوان host داخلي.
- يطمح الـ attacker أن يكون استخدامه للعنوان المزور سيسمح له باختراق الأنظمة التي تكون فيها سرية بسيطة على الـ (source address).
- و الإجراء المضاد في هذه الحالة هو التخلي عن الـ (packets) التي تحتوي على (source address) داخلي في حال أن هذه الـ (packet) قادمة من (interface) خارجية.

الهجمة الثانية : هجمات تسير المصدر (Source routing attacks):

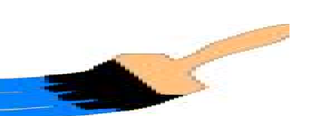
- تقوم الـ (source station) بتحديد المسار الذي يجب على الـ (packet) سلوكه عند مرورها في الإنترنت، على أمل أن ذلك سيتجاوز إجراءات السرية التي لا تقوم بتحليل معلومات تسيير الـ (source).
- الإجراء المضاد في هذه الحالة هو التخلي عن كل الـ (packets) التي تستخدم هذا الخيار.

الهجمة الثالثة : هجمات الجزء الصغير جداً (Tiny fragment attacks):

- يستخدم الـ (intruder) خيار تجزئة الـ IP (IP fragmentation option) و ذلك بغرض توليد (fragments) صغيرة جداً ، و جعل معلومات الـ (TCP header) في (packet fragment) منفصل.
- هذه الهجمة صممت لمراوغة قواعد التنقية (Filtering rules) و التي تعتمد على معلومات الـ (TCP header).
- يطمح الـ (Attacker) أن الـ (Filtering router) سيقوم فقط باختبار أول (fragment) بينما ستمر بقية الـ (fragments) دون اختبار.
- الإجراء المضاد في هذه الحالة هو التخلي عن كل الـ (packets) التي يكون نوع البروتوكول فيها هو الـ (TCP) و ازاحة الـ (IP fragment) له مساوية للواحد الصحيح.

النوع الثاني : بوابات المستوى التطبيقي (Application-level gateways):

- يسمى أيضاً بالـ (proxy server) و يعمل كناقل لمرور المستوى التطبيقي (Application-level traffic).
- يتصل المستخدم بالـ (gateway) باستخدام تطبيق من تطبيقات الـ (TCP/IP)، مثل الـ (Telnet) أو الـ (FTP).
- تطلب الـ (gateway) من المستخدم إدخال اسم الـ (host) البعيد المراد الوصول إليه.
- عندما يستجيب المستخدم بتزويده للـ (UserID) و معلومات التحقق الصحيحة، فإن الـ (gateway) تتصل بالتطبيق الموجود على الـ (host) البعيد و تنقل أجزاء الـ (TCP) التي تحتوي على بيانات التطبيق بين النهايتن الطرفيتين.
- إذا لم تقدم الـ (gateway) شفرة الـ (proxy) لتطبيق محدد ، فإن الخدمة لن تكون مدعومة و لن يتم إرسالها عبر الـ (Firewall).

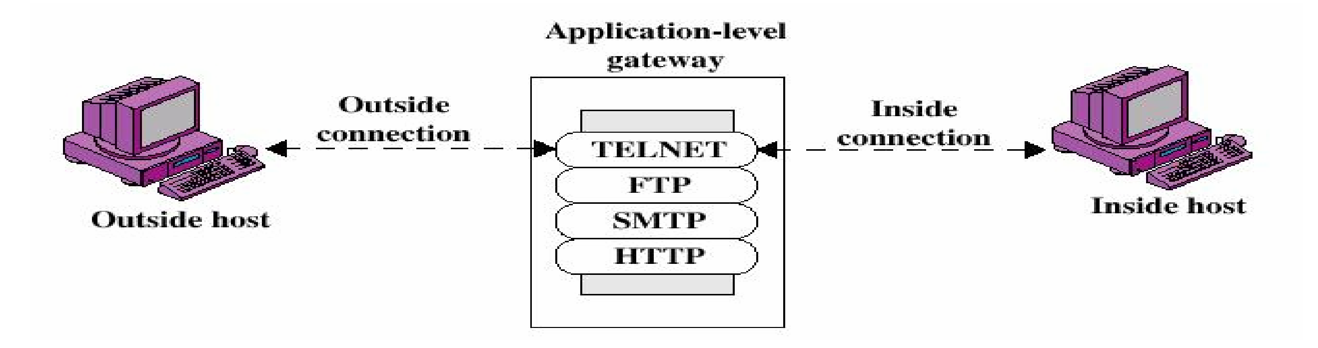


مزايا بوابات المستوى التطبيقي (Advantages of Application-level gateways):

- أكثر سرية من النوع السابق (Higher security than packet filters).
- يحتاج فقط للفحص الدقيق للقليل من التطبيقات المسموحة (Only need to scrutinize a few allowable applications).
- من السهل تسجيل و تدقيق كل المرورات القادمة (Easy to log and audit all incoming traffic).

مساوئ بوابات المستوى التطبيقي (Disdvantages of Application-level gateways):

- الحاجة إلى زيادة معالجة إضافية لكل إرتباط (Additional processing overhead on each connection (gateway as splice point)).

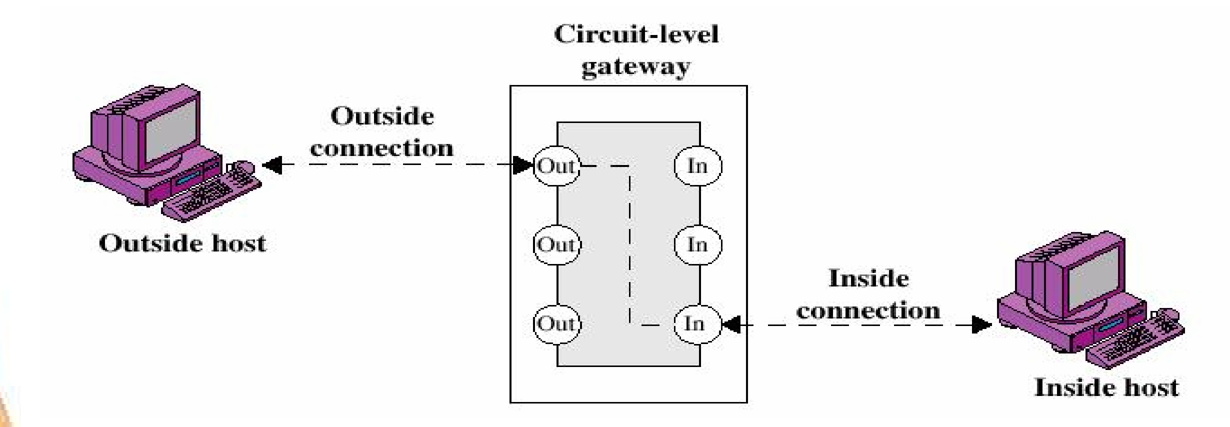


النوع الثالث : بوابات على مستوى الدائرة (Circuit-level gateways).

- يمكن أن يكون هذا النوع نظاماً مستقلاً (stand-alone system) أو وظيفة مخصصة (specialized function) يتم إنجازها بواسطة (Application-level Gateway).
- لا يسمح بارتباطات الـ (end-to-end TCP)، و بدلاً عن ذلك يقوم بوضع اثنين من ارتباطات الـ (TCP):

  أحدهما بين الـ (gateway) نفسها و مستخدم الـ (TCP) على الـ (host) الداخلي.

  و الآخر بين الـ (gateway) نفسها و مستخدم الـ (TCP) على الـ (host) الخارجي.
- عندما يتم إنشاء هذين الارتباطين فإن الـ (gateway) ستقوم بنقل الـ (TCP segments) من ارتباط إلى آخر دون فحص المحتويات.
- تكون وظيفة السرية هنا هي تحديد أي من الاتباطات سيسمح لها.
- يستخدم هذا النوع في حالة أن يكون مدير النظام واثقاً من المستخدمين الداخليين.
- من الأمثلة عليه الـ (SOCKS package).





<u>مضيف الحصن (Bastion host):</u>

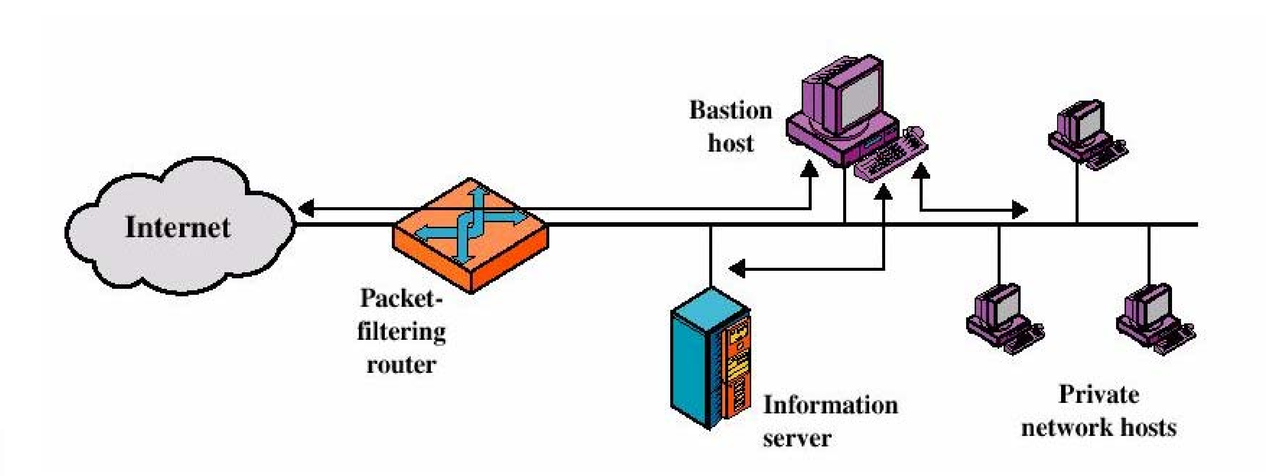
- و هو نظام معرف من قبل مدير الـ (Firewall) كنقطة حرجة قوية في سرية الشبكة.
- يعمل الـ (Bastion host) كبيئة لأيٍ من الـ (application-level gateway) أو الـ (circuit-level gateway).

<u>إعداد جدار النار (Firewall configuration):</u>

- بالإضافة إلى استخدام التهيئة البسيطة لنظام وحيد (single packet filtering router or single gateway)، فإن هناك أنواع تهيئة أكثر تعقيداً.
- سنتطرق هنا إلى أكثر ثلاثة تهيئات شيوعاً:

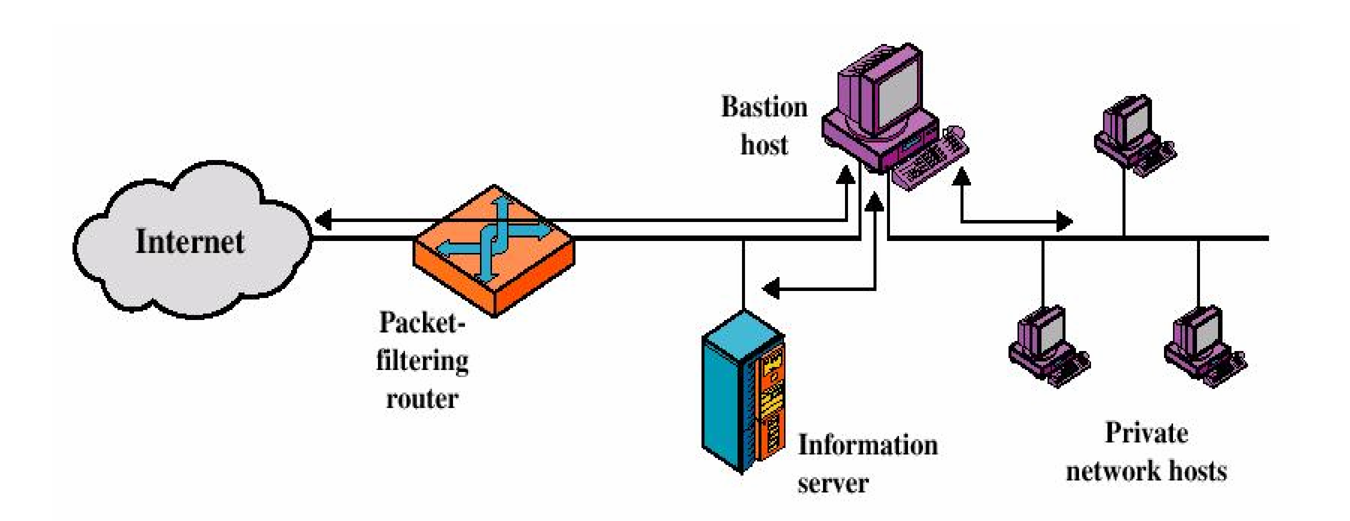
<u>التهيئة الأولى : الـ Screened host firewall system (single-homed bastion host):</u>

- يتكون الـ (Firewall) من نظامين :
  (*) الـ (packet-filtering router).
  (*) الـ (Bastion host).
- يتم تهيئة الـ (router) بحيث :
  1. فيما يخص الـ (traffic) القادم من الانترنت ، يسمح فقط للـ (IP packets) المخصصة للـ (Bastion host).
  2. فيما يخص الـ (traffic) من الشبكة الداخلية، يسمح فقط للـ (IP packets) القادمة من الـ (Bastion host).
- يقوم الـ (Bastion host) بإنجاز عمليات الـ (authentication) و الـ (proxy functions).
- السرية هنا أفضل مما هو عليه الحال في الـ (single configuration) و ذلك لسببين:
  1. أن هذا الـ (configuration) ينفذ كلاً من الـ (packet-level filtering) و الـ (application-level filtering) و يسمح بالمرونة عند تعريف سياسة السرية.
  2. يجب على الـ (intruder) بشكل عام أن يخترق نظامين منفصلين.
- أيضاً تتوافر هنا المرونة في تزويد الوصول المباشر إلى الإنترنت (خادم المعلومات العام ، مثل الـ web server).



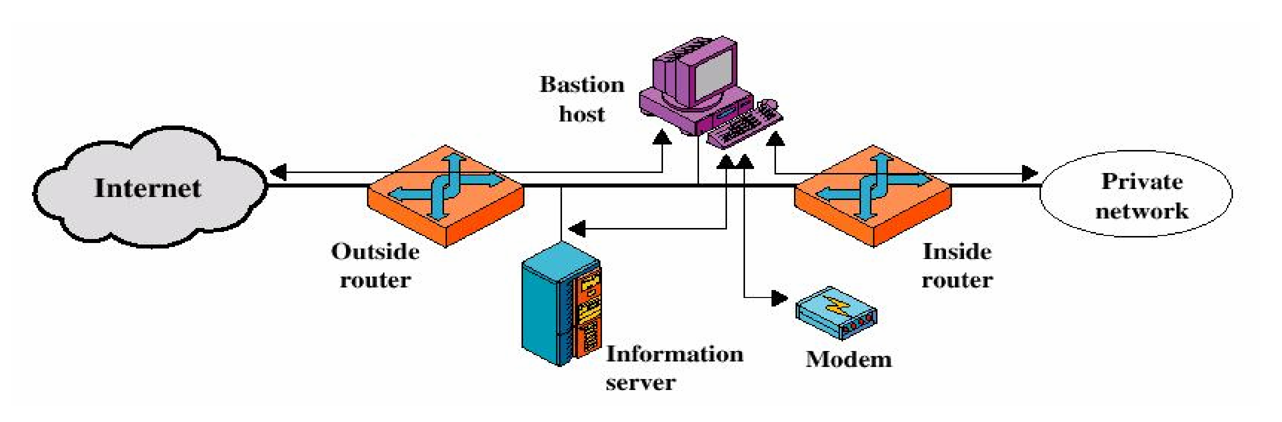
التهيئة الثانية : الـ (Screened host firewall system (dual-homed bastion host)):

- لا يفضح الـ (packet-filtering router) بشكل كامل.
- يجب أن يتدفق الـ (traffic) بين الانترنت و الـ (hosts) الآخرين في الشبكة الخاصة عبر الـ (Bastion host).



التهيئة الثالثة : الـ (Screened-subnet firewall system):

- أكثر الثلاثة الـ (configurations) أمناً.
- يتم استخدام اثنين من الـ (packet-filtering routers).
- يتم توليد شبكة جزئية (sub-network) معزولة.



مزايا هذا النوع :

- ❖ يوجد ثلاثة مستويات من الحماية لإحباط الـ (intruders).
- ❖ يعلن الـ (router) الخارجي في الانترنت فقط عن وجود الـ (screened subnet)، بمعنى أن الشبكة الداخلية تكون غير مرئية على شبكة الانترنت.
- ❖ يعلن الـ (router) الداخلي في الشبكة الداخلية فقط عن وجود الـ (screened subnet)، بمعنى أن الأنظمة على الشبكة الداخلية لا يمكن أن تنشئ مسارات مباشرة إلى شبكة الانترنت.